JIANGSU UNIVERSITY, SCHOOL OF COMPUTER SCIENCE AND COMMUNICATION ENGINEERING

Cryptography_exercise

Students

November 4, 2016

1. A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p , substitute the ciphertext letter C:

$$C = E([a, b], p) = (ap + b) \bmod 26 \quad .$$

A basic requirement of any encryption algorithm is that it be one-to-one. That is, if p≠q,then E(k,p)≠E(k,q) . Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a=2 and b=3,then E([a,b],0)=E([a,b],13)=3. a. Are there any limitations on the value of b Explain why or why not. b. Determine which values of are not allowed. c. Provide a general statement of which values of a are and are not allowed. Justify your statement.

ANSWER:a.No. A change in the value of b shifts the relationship between plaintext letters and ciphertext letters to the left or right uniformly, so that if the mapping is one-to-one it remains one-to-one. b.2,4,6,8,10,12,13,14,16,18,20,22,24. Any value of a larger than 25 is equivalent to a mod 26. c.The values of a and 26 must have no common positive integer factor other than 1. This is equivalent to saying that a and 26 are relatively prime, or that the greatest common divisor of a and 26 is 1. To see this, first note that E(a,p) = E(a,q) (0≤p≤q<26) if and only if a(p-q) is divisible by 26. 1.Suppose that a and 26 are relatively prime. Then, a(p-q) is not divisible by 26, because there is no way to reduce the fraction a/26 and (p-q) is less than 26. 2.Suppose that a and 26 have a common factor k>1. Then E(a,p)=E(a,q), if q=p+m/k≠p.

2. A ciphertext has been generated with an affine cipher.The most frequent letter of the ciphertext is B, and the second most frequent letter of the ciphertext is U. Break this code.

ANSWER:Assume that the most frequent plaintext letter is e and the second most frequent letter is t. Note that the numerical values are e = 4; B = 1; t = 19; U = 20. Then we have the following equations:

$$1 = (4a + b) \bmod 26$$
$$20 = (19a + b) \bmod 26$$

Thus, 19 = 15a mod 26. By trial and error, we solve: a = 3. Then 1 = (12 + b) mod 26. By observation, b = 15.

3. One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Typically, at least in spy novels, the first sentence of a book serves as the key. The particular scheme discussed in this problem is from one of the best suspense novels involving secret codes, Talking to Strange Men, by Ruth Rendell. Work this problem without consulting that book!Consider the following message:

SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

This ciphertext was produced using the first sentence of The Other Side of Silence(a book about the spy Kim Philby):The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars.
A simple substitution cipher was used.
a. What is the encryption algorithm?
b. How secure is it?
c. To make the key distribution problem simple, both parties can agree to use the first or last sentence of a book as the key. To change the key, they simply need to agree on a new book. The use of the first sentence would be preferable to the use of the last. Why?

ANSWER:a.The first letter t corresponds to A, the second letter h corresponds to B, e is C, s is D, and so on. Second and subsequent occurrences of a letter in the key sentence are ignored. The result:
ciphertext: SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
plaintext: basilisk to leviathan blake is contact
b. It is a monalphabetic cipher and so easily breakable.
c. The last sentence may not contain all the letters of the alphabet. If the first sentence is used, the second and subsequent sentences may also be used until all 26 letters are encountered.

4. Using the VigenÍÍre cipher, encrypt the word ąřexplanationąś using the key leg.

ANSWER:key: legleglegle
plaintext: explanation
ciphertext: PBVWETLXOZR

5. It can be shown that the Hill cipher with the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{0.1}$$

requires that is relatively prime to 26; that is, the only common positive integer factor of and 26 is 1. Thus, if or is even, the matrix is not allowed. Determine the number of different (good) keys there are for a 2 ąÁ 2 Hill cipher without counting them one by one, using the following steps:
a. Find the number of matrices whose determinant is even because one or both rows are even. (A row is ąřevenąś if both entries in the row are even.)
b. Find the number of matrices whose determinant is even because one or both columns are even. (A column is ąřevenąś if both entries in the column are even.)
c. Find the number of matrices whose determinant is even because all of the entries are odd.
d. Taking into account overlaps, find the total number of matrices whose determinant is even.
e. Find the number of matrices whose determinant is a multiple of 13 because the first column is a multiple of 13.
f. Find the number of matrices whose determinant is a multiple of 13 where the first column is not a multiple of 13 but the second column is a multiple of the first modulo 13.
g. Find the total number of matrices whose determinant is a multiple of 13.
h. Find the number of matrices whose determinant is a multiple of 26 because they fit cases parts (a) and (e), (b) and (e), (c) and (e), (a) and (f), and so on.
i. Find the total number of matrices whose determinant is neither a multiple of 2 nor a multiple of 13.

ANSWER:
a.7×13^4
b.7×13^4
c.13^4
d.10×13^4
e.24×13^2
f.$24\times (13^2$-1)
g.37648
h.23530
i.157248

6. Consider a Feistel cipher composed of sixteen rounds with a block length of 128 bits and a key length of 128 bits. Suppose that, for a given k,the key scheduling algorithm determines values for the first eight round keys,k1,k2 and then sets:

k9=k8,k10=k7,k11=k6.....k16=k1

Suppose you have a ciphertext c. Explain how, with access to an encryption oracle,you can decrypt c and determine m using just a single oracle query. This shows that such a cipher is vulnerable to a chosen plaintext attack. (An encryption oracle can be thought of as a device that, when given a plaintext, returns the corresponding ciphertext. The internal details of the device are not known to you and you cannot break open the device. You can only gain information from the oracle by making queries to it and observing its responses.)

ANSWER:Because of the key schedule, the round functions used in rounds 9 through 16 are mirror images of the round functions used in rounds 1 through 8. From this fact we see that encryption and decryption are identical. We are given a ciphertext c. Let m' = c. Ask the encryption oracle to encrypt m'. The ciphertext returned by the oracle will be the decryption of c.